REMARKS

The Examiner has rejected Claims 1-29 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-29 of U.S. Patent No. 6,839,852. Applicant has submitted herewith a terminal disclaimer in order to overcome such rejection.

The Examiner has rejected Claims 1-29 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner has stated that Claims 1, 8-10, 19-22 and 23-25 recite a "subset of the plurality of computers" and that Claims 25 recites a "similar phrase sent across the subset of the plurality of client computers" and that neither are described in the specification. Applicant respectfully disagrees.

Specifically, with respect to applicant's claimed "subset of the plurality of computers," applicant respectfully points out the following excerpts from page 8, line 19-page 9, line 21 in the specification:

> "As shown in Figure 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation **302**. ...
> Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation **302**. ...
> By way of example, if it is found that a large number of computers are the subject of the same port scans, this may be assumed to indicate intrusion activity. In another example, if a large number of computers receive an email with the phrase "OPEN ATTACHMENT" in the subject header, this too may be considered intrusion activity."

Clearly, as noted from the excerpt above, collecting information from a plurality of computers, and identifying similar activity across a subset (e.g. large number, etc.) of computers is indeed supported. In addition, applicant respectfully points out that the

above cited excerpt from the specification clearly states that "if a large number of computers receive an email with the phrase 'OPEN ATTACHMENT' in the subject header, this too may be considered intrusion activity." Thus, applicant's Claim 25 requiring a technique "wherein the similar intrusion activity includes an e-mail with a similar phrase sent across the subset of the plurality of client computers" is also clearly supported by the specification.

The Examiner has rejected Claims 1-29 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner has stated that the term "similar" in Claims 1-3, 8-10, 19-22, 24 and 25 is a relative term which renders the claim indefinite.

Applicant respectfully disagrees and points out page 9, lines 9-21 in the specification, which states that "the information may be analyzed for patterns that are indicative of intrusion activity" and that, for example, "if it is found that a large number of computers are the subject of the same port scans, this may be assumed to indicate intrusion activity" or "if a large number of computers receive an email with the phrase 'OPEN ATTACHMENT'" in the subject header, this too may be considered intrusion activity." Thus, applicant's claimed "similar intrusion activity" is not indefinite, since the specification clearly states that the information is analyzed for patterns indicative of intrusion activity, which is clearly an example of "similar intrusion activity."

The Examiner has maintained the rejection of Claims 1-29 under 35 U.S.C. 102(b) as being anticipated by Conklin et al. (U.S. Patent No. 5,991,881). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 8-10 and 19-22, the Examiner has relied on the Summary and Col. 3, lines 37-43 et al. in Conklin to make a prior art showing of applicant's claimed "establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting

information relating to intrusion activity" (see the same or similar, but not necessarily identical language in each of the independent claims). Applicant respectfully asserts that Conklin only discloses "Intrusion Detection portions of a Network Surveillance System." Applicant further notes that Figure 4 of Conklin shows a single intrusion detection block in communication with an operating system of a single computer, and not "a plurality of computers with firewalls," as specifically claimed by applicant (emphasis added).

In the latest Office Action dated 2/7/2006, the Examiner has argued that Conklin discloses "a system and method for network surveillance and detection of attempted intrusions, or intrusions, into the network and into computers connected to the network." Applicant respectfully asserts that Conklin only teaches a "Network Surveillance System [that] captures all traffic broadcast on the segment...[including] the communications between Host A and Host C" (see Col. 2, lines 48-50). In addition, Conklin teaches that the "Network Surveillance System operates through a computer, attached to the network" (Col. 3, lines 44-46). However, applicant respectfully asserts that Figures 1-3 in Conklin clearly show the Network Surveillance unit being a single unit separate from the hosts for which traffic is being captured, and that the Network Surveillance unit merely sits on a communication segment for capturing data transmitted on such segment. Thus, Conklin's Network Surveillance system, which is separate from such computers, cannot meet applicant's claimed "plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity" (emphasis added), in the context claimed.

Still with respect to applicant's claimed "establishing network communications between a server computer and a plurality of client computers with firewalls over a network," the Examiner has also, in his latest response to remarks, relied on Col. 3, lines 36-65 and Col. 4, lines 9-28 in Conklin to make a prior art showing of such claim language. Applicant again respectfully asserts that the Conklin excerpts fail to teach "a plurality of client computers with firewalls," as claimed. As argued above, Conklin only discloses a Network Surveillance System that is separate from the host computers and that collects data transmitted between the host computers. In fact, applicant points out

that as shown in Figures 1 and 2, the Network Surveillance System is located on an Ethernet segment and collects data transmitted on that Ethernet segment. Furthermore, as shown in Figure 3, the Network Surveillance System is attached to a router, and not the host computers. Thus, clearly the cited Conklin excerpts do not meet applicant's claimed "plurality of client computers with firewalls" (emphasis added), in the context claimed.

In addition, the Examiner has relied on Col. 4, line 45-Col. 5, line 45 et al. to make a prior art showing of applicant's claimed technique "wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned addresses" (emphasis added). Applicant respectfully asserts that the only mention of addresses in such excerpts merely relates to developing network specific characteristics or facts, including "common destination/source address combinations." Further, only when network traffic is outside normal tolerances for such measured characteristics is action taken. Clearly, only maintaining data on common destination/source address **combinations** in order for such combinations to be compared against thresholds, as in Conklin, does not even suggest "a list of trusted and banned addresses," as applicant claims.

With respect to independent Claim 1 et al., the Examiner has relied on the Summary, Col. 4, lines 9-29 and Col. 5, lines 25-61 in Conklin to make a prior art showing of applicant's claimed technique "wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response." As argue above, applicant respectfully asserts that Conklin only teaches a single Network Surveillance System. Furthermore, such single unit consists of multiple components, as shown in Figure 6. In addition, Conklin discloses a "second logging function" of the Network Surveillance unit that "is used to hold all ensuing packets associated with...reportable activity...by any one of its identifiable characteristics" (see Col. 5, lines 35-44). Thus, in Conklin, only the single Network Surveillance unit captures packets communicated between client computers, which clearly does not meet applicant's claimed "firewalls [on the plurality of client computers

that] are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response," when read in context.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Conklin reference, as noted above. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P095/02.014.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100